

## UNITED STATES DISTRICT COURT

for the  
District of Oregon

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*

Case No. 3:20-mc-01158

The person of Gilbert J. Paniagua, his cell phone, and  
the premises located at 8338 N. Interstate Ave., Apt.  
412, Portland, OR, all as described in Attachment A

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The person of Gilbert J. Paniagua, his cell phone, and the premises located at 8338 N. Interstate Ave., Apt. 412, Portland, OR, all as more fully described in Attachment A  
located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B)	Transportation, distribution, receipt, possession of, and accessing with intent to view child pornography

The application is based on these facts:

See the attached affidavit of HSI Special Agent William M. Bergin.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days *(give exact ending date if more than 30 days)*: \_\_\_\_\_ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

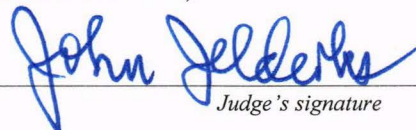
HSI SA William Bergin

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone at 3:15 a.m. *(specify reliable electronic means)*.

Date:

November 10, 2020
  
*Judge's signature*
City and state: Portland, Oregon

Hon. John Jelderks, United States Magistrate Judge

*Printed name and title*

## **ATTACHMENT A**

### **Description of the Person, Premises, and Property to be Searched**

#### **1. Person**

The person of Gilbert J. PANIAGUA (and any cell phone or digital device on his person at the time of search provided that he is located in the District of Oregon at the time of search), date of birth XX/XX/1989; a male with brown hair and hazel eyes, approximately 5'7" and 268 lbs.



#### **2. Subject Premises**

The residence is located at 8338 N. Interstate Avenue, Apt 412, Portland, Oregon. The residence is a four-story apartment complex, black and white in color. The complex has a secure parking garage in the rear of the building. The numbers "8338" can clearly be seen on the front door.



#### **3. Subject Cell Phone**

PANIAGUA's cell phone. Make/Model is currently unknown, however, the telephone number 360-451-6956 and/or the International Mobile Subscriber Identity(s) (IMSI) (310120232561560), can be verified in the phone's settings when the warrant is executed.

## **ATTACHMENT B**

### **Items to be Searched For, Seized, and Examined**

The following items, documents, and records that contain evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2252A(a)(1), (a)(2), and (a)(5)(B) including:

#### **I. Digital Evidence**

1. The cellular telephone described in Attachment A, and any mobile devices that may have been used to facilitate violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B);
2. Any computers that may have been used to facilitate violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B), including any peripheral devices such as external hard drives, external disk drives, power supplies, modem, and routers;
3. Any computer equipment or digital devices that are capable of being used to create, access, or store contraband or evidence, fruits, or instrumentalities of such crimes, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and security devices;
4. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store contraband or evidence, fruits, or instrumentalities of such crimes;



5. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, thumb drives, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store contraband, or evidence, fruits, or instrumentalities of such crimes;

6. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

7. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

8. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

9. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, digital devices, storage devices, or data; and

10. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage;



and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

## **II. Records, Documents, and Visual Depictions**

11. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

12. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

13. Any motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

14. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

15. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

16. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

17. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs;

18. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received.

19. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and or notes associated with child pornography or those who collect, disseminate, or trade in child pornography;

As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.

#### **Search Procedure**

20. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, “computer personnel”), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and herein.

b. *On-site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and herein. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date the warrant was executed. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at



trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date the warrant was executed. The government shall complete the search of the digital device or image within 180 days of the date the warrant was executed. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

STATE OF OREGON                    )  
  ) ss:                   AFFIDAVIT OF WILLIAM M. BERGIN  
County of Multnomah                )

**Affidavit in Support of an Application for a Search Warrant**

I, William M. Bergin, being duly sworn, do hereby depose and state as follows:

**Introduction and Agent Background**

1.     I am a Special Agent and a certified computer forensic agent with the U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI). I have been employed as a Special Agent for approximately 18 years. I am currently assigned to the child exploitation unit at the HSI office in Portland, Oregon. Previously, I was assigned to the ICE/HSI Office in Reno, Nevada, where I worked for over 18 years investigating various crimes, including child exploitation offenses. My formal law enforcement training includes successfully completing the U.S. Customs Special Agent basic training course at the Federal Law Enforcement Training Center in Glynco, Georgia, and the Basic Computer Evidence Recovery Training (BCERT) course at the HSI Cyber Crimes Center. I hold an “A+” certification which certifies skills in entry-level PC technology. It is a vendor-neutral certification, with an emphasis on the expertise needed to work as a computer service technician, troubleshooting and repairing PCs.

2.     I have assisted federal and state partners during their investigations. As such, I have become familiar with the ways in which child pornography is produced, distributed, and/or possessed, including through the use of various social media websites, apps, and “cloud” based storage. Those social media sites include Facebook, Twitter, Kik, Snapchat, Discord, and others. Often times, individuals involved in child exploitation will collect or store images and/or videos in offsite locations such as cloud-based storage to avoid detection by law

enforcement. At other times, individuals store child pornography on various media devices they keep at their residence. I have also become familiar with jargon or slang terms that people involved in child exploitation use to discuss their activities.

3. I have worked with agents involved in numerous investigations involving the sexual exploitation of children or the distribution, receipt, and possession of child pornography. I have participated in searches of premises and assisted in gathering evidence pursuant to search warrants, including search warrants in multiple child pornography investigations.

4. I submit this affidavit in support of an application for a search warrant authorizing searches of the **person of Gilberto J. PANIAGUA**, the **Subject Premises** located at 8338 N. Interstate Avenue, Apt. 412, Portland, OR 97217, and **PANIAGUA's Cell Phone**, as described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B) (involving the transportation, distribution, possession, and accessing with intent to view child pornography), as described in Attachment B.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.



**Applicable Law**

6. *Title 18 U.S.C. § 2252A(a)(1)* makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

7. *Title 18 U.S.C. § 2252A(a)(2)* makes it a crime to knowingly receive or distribute any child pornography using any means or facility of interstate or foreign commerce, or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. *Title 18 U.S.C. § 2252A(a)(5)(B)* makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term “child pornography” is defined in 18 U.S.C. § 2256(8).

**Background on Computers and Child Pornography**

9. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

10. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

11. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and

distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

12. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously in the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on someone's person or inside their vehicle.

13. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs such as LimeWire and eMule, and networks such as Gnutella, Tumblr, and BitTorrent, among others. Collectors and distributors of child pornography also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up and access an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer and other digital devices.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

***Kik Messenger Application Explained***

15. Kik is an instant messaging mobile application from MediaLab available free of charge on iOS and Android operating systems. It uses a smartphone's data plan or Wi-Fi to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content after users register a username. Kik is known for its features preserving users' anonymity, such as allowing users to register using an email address without providing a telephone number. However, the Kik application logs user IP addresses, which can be used to determine a user's location.

16. Kik allows users to chat either individually or in public or private groups. In addition, users can exchange images, videos, sketches, stickers, and more with mobile web pages. Kik can be used on multiple mobile devices, including cellular phones and tablets.



17. In general, providers like Kik ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an email address. However, Kik does not verify the accuracy of the information subscribers provide.

18. Kik users create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is displayed in their Kik profile.

***Background Information on People who Possess and Collect Child Pornography***

19. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence or vehicle, and on computers and digital storage media under their direct control. They may also maintain their collections in secure offsite locations, such as an online cloud storage account. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

20. I also know from my training and experience that persons who download child pornography from the Internet, and those who collect child pornography, frequently save images and videos of child pornography on their computers and/or transfer copies to other computers and data storage media, including external hard drives, thumb drives, flash drives, SD cards, and CDs or DVDs. Moreover, it is common in child pornography investigations to find child pornography on multiple devices and/or data storage media kept at their residence, in their vehicles, and on their person, rather than on any single device.

21. I know based on my training and experience that many social media applications, such as Facebook, Instagram, Kik, Twitter, and others can be directly accessed and used with one's cellular phone. Often times, these applications require the user to download the application directly to their phone, which then allows seamless use between the cellular phone and the social media website.

### **Statement of Probable Cause**

#### ***HSI Investigations in Tennessee and Michigan***

22. On June 10, 2020, an HSI special agent in Chattanooga, Tennessee, who was online in the Kik application in an undercover capacity, observed a user post a child pornography video depicting an adult male sexually assaulting an infant. The undercover agent (UCA) reached out to the user who posted the video and asked for information about it. The user claimed that he was the adult male featured in the video and that the infant was the daughter of a friend.

23. On June 11, 2020, the UCA determined that this user was located in or near Detroit, Michigan, and asked HSI Detroit for assistance. HSI Detroit's investigation revealed that the owner of this Kik account was most likely John David LEWIS, who resided in either

Allen Park, Michigan, or Toledo, Ohio. HSI Detroit applied for search warrants for both addresses and executed them simultaneously on the evening of June 12, 2020.

24. LEWIS was determined to reside at the address in Toledo, Ohio, having recently moved there from the address in Allen Park, MI. During an interview with HSI Detroit special agents, LEWIS admitted to producing, distributing, receiving, and possessing child pornography. LEWIS admitted to being the adult male subject in the video observed by the UCA and confirmed the identity of the minor victim (referred to herein as MV-1). LEWIS was arrested and charged with producing, distributing, receiving, and possessing child pornography.

25. Agents seized several electronic devices during the execution of the warrant, including an iPhone SE belonging to LEWIS. A forensic examination of the phone revealed approximately 49 videos and 21 images that met the federal definition of child pornography. Some of the videos depicted the sexual abuse of children as young as infants. A number of the images and videos were found within the Kik app file path  
\\mobile\\Containers\\Shared\\AppGroup\\group.com.kik.chat\\cores\\private. The forensic examiner noted that the Kik application on the iPhone SE had the username “chancebandet,” and a display name of “J L.” HSI SA Dave Alley saw numerous chats in the Kik app that involved discussing and trading child pornography.

26. SA Alley observed chats between LEWIS and a Kik user with the username “MapsMaps89.” SA Alley noted the following:

- LEWIS sent user MapsMaps89 the video of himself sexually assaulting MV-1.
- LEWIS sent user MapsMaps89 an image of MV-1’s vagina.
- LEWIS sent user MapsMaps89 child pornography depicting other children.
- User MapsMaps89 sent LEWIS child pornography.



27. On June 19, 2020, SA Alley served a summons on Kik for subscriber information for user MapsMaps89. Kik responded to this request and provided subscriber information and IP connection information for user MapsMaps89, which included numerous connections with the IP address 24.21.207.131.

28. That IP address belongs to Comcast Communications. On August 17, 2020, SA Alley served a summons on Comcast for subscriber information for IP address 24.21.207.131, port 55468. Comcast provided the following information in response to the summons:

- Subscriber Name: Bert PANIAGUA
- Service Address: 8338 N. Interstate Avenue, Apt 412, Portland, OR (the **Subject Premises**)
- Billing Address: 8338 N. Interstate Avenue, Apt 412, Portland, OR
- Telephone #: 360-451-6956 (**PANIAGUA's Cell Phone**)
- Start of Service: 06/01/2019
- Account Status: Active

***Investigation Forwarded to HSI Portland***

29. Based on the fact that the Kik account "MapsMaps89" was being accessed from an IP address in Portland, Oregon, HSI Detroit asked HSI Portland to continue the investigation. HSI Detroit sent me the Kik message exchanges between LEWIS and "MapsMaps89," which as described below, I believe is used by **PANIAGUA**.

30. On September 18, 2020, pursuant to an administrative subpoena, Portland General Electric provided the following utility records for the **Subject Premises**:

- a. Current Customer: Gilberto J. Paniagua
- b. Contact Number: 360-451-6956 (**PANIAGUA's Cell Phone**)
- c. Date of Birth: xx/xx/89
- d. Email: [bertjames89@yahoo.com](mailto:bertjames89@yahoo.com)
- e. Start Date: 6/17/2019

31. On September 21, 2020, pursuant to an administrative subpoena, the apartment complex at 8338 N. Interstate Avenue provided current rental records for the **Subject Premises**. During my review of the rental records, I learned that the **Subject Premises** were rented by **PANIAGUA** on May 30, 2019. He is the current lease holder until April 30, 2021. Additionally, on his 2019 and 2020 rental applications, **PANIAGUA** provided the telephone number 360-451-6956 (**PANIAGUA's Cell Phone**), an email address of [bertjames89@yahoo.com](mailto:bertjames89@yahoo.com), and stated that he is currently employed by Amazon. **PANIAGUA** provided records that confirmed that he was selling a residence located at 1022 E 57<sup>th</sup>, Tacoma, WA 98404 in order to move to Portland to accept his new position with Amazon. According to the lease, **PANIAGUA** is the only occupant of the apartment, and provided a Washington driver's license that was issued on December 23, 2015, and which listed an address of 1202 N Fife Street, Tacoma, WA 98406. Based on the date of issue and the fact that **PANIAGUA** provided a different address for the home that he owned, I believe that 1202 N Fife Street, Tacoma, WA 98406 is a former residence and that he never updated the address on his Washington driver's license.

32. On September 24, 2020, pursuant to an administrative subpoena, Sprint provided subscriber records for 360-451-6956 (**PANIAGUA's Cell Phone**). That number is subscribed to **PANIAGUA** at 1202 N Fife Street, Tacoma, WA 98406, the same address as listed on **PANIAGUA's** Washington driver's license. The subscriber records were last updated in April 2019.

33. During my review of the Kik chat messages between John LEWIS and MapsMaps89, I saw several images and one video that were distributed by both LEWIS and

MapsMaps89 during a messaging exchange on June 7, 2020, which met the federal definition of child pornography. The following are descriptions of some of the images and the video:

- LEWIS sent user MapsMaps89 the video of himself sexually assaulting MV-1 (minor victim) by putting his penis into the mouth of a baby that appears to be approximately 4-6 months old, until the baby starts to choke.
- LEWIS sent user MapsMaps89 an image of what appears to be the vagina of a female child who is approximately six months to one year old. The child appears to be wrapped in a white blanket.
- User MapsMaps89 sent LEWIS an image of what appears to be an adult female licking the erect penis of a boy who appears to be approximately 1-2 years old.
- User MapsMaps89 sent LEWIS an image of a young girl who appears to be approximately 1-2 years of age. The girl's legs are spread apart; her vagina and anus are the primary focus of the image. The girl's face and naked body are visible as well.
- User MapsMaps89 sent LEWIS an image of a young girl who appears to be approximately 1-3 years old. The girl is laying naked on her back with her legs spread apart. An adult's finger appears to be attempting to penetrate the girl's vagina.
- User MapsMaps89 sent LEWIS an image of a young girl who appears to be approximately 1-3 year of age. The image shows the lower half of the girl, who is naked from the waist down, and is focused on her vagina and anus. What appears to be an adult female wearing a "strap-on" dildo is penetrating the girl's anus.



***PANIAGUA Previously Identified as Distributing Child Pornography***

34. During my review of additional law enforcement records, I learned that **PANIAGUA** was identified in at least two other investigations involving the receipt and/or distribution of child pornography. I have not personally reviewed any of the images or videos involved in those investigations.

35. Law enforcement records revealed that **PANIAGUA** was identified as a Kik user with screen name “mashami89” that was suspected of sharing suspected child pornography via the Kik app in approximately August of 2019. That Kik account was subscribed to **PANIAGUA** at the **Subject Premises** with a reported phone number of 360-451-6956 (**PANIAGUA’s Cell Phone**).

36. **PANIAGUA** was also suspected of using the Kik app on March 19, 2019, to share child pornography under the Kik username of “bertofsleep” with an email address of [bertjames89@yahoo.com](mailto:bertjames89@yahoo.com) (**PANIAGUA’s** middle name is James and his year of birth is 1989). **PANIAGUA** provided that same email address on his rental application for the **Subject Premises** and is on the electric utility records for the **Subject Premises**. The child pornography was suspected of being uploaded from an IP address belonging to Comcast. In response to an administrative summons, Comcast stated that the subscriber of that IP address was Allison **PANIAGUA**, who is believed to be **PANIAGUA’s** sister.

37. The **Subject Premises** is described as a four-story apartment complex, black and white in color. The residence is located at 8338 N. Interstate Avenue, Apt 412, Portland, Oregon. The complex has a secure parking garage in the rear of the building. The numbers “8338” can clearly be seen on the front door.

### **Search and Seizure of Digital Data**

38. This application seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

39. Based on my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

### **Removal of Data Storage Devices**

40. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during a search of premises it is not always possible to create a forensic image of or search digital devices or media for data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all of the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it is generally highly impractical to search for data during the execution of a physical search of premises. Storage devices capable of storing 500 gigabytes to several terabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive. The larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can become impractical.

**Laboratory Setting May Be Essential for Complete and Accurate Analysis of Data**

41. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

42. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the



examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

43. *Latent Data:* Searching digital devices can require the use of precise scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's

operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

44. *Contextual Data:*

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and

times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user, can point toward the existence of evidence in other locations, and can also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software, may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

#### **Search Procedure**

45. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:



a. *On site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, “computer personnel”), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

b. *On site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law

enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date the warrant was executed. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to the warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date the warrant was executed. The government shall complete the search of the digital device or image within 180 days of the date the warrant was executed. If the government needs additional time to complete the search, it may seek an extension of time from the Court.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data that fall within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized

pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

#### **Items to be Seized**

46. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as thumb drives and other USB data storage devices, floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants,



iPods, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess, or view child pornography, including the web browser's history; temporary Internet files; cookies, bookmarked or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

### **Retention of Image**

47. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

### **Inventory and Return**

48. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

49. The government has made no prior effort in any judicial forum to obtain the materials sought in this requested warrant.

### **Conclusion**

50. Based on the foregoing, I have probable cause to believe that **PANIAGUA** committed violations of 18 U.S.C. §§ 2252A (a)(1), (a)(2), and (a)(5)(B), and that contraband and evidence, fruits, and instrumentalities of those violations will be located on his person, at the **Subject Premises**, and on in his cell phone, all as described in Attachment A. I therefore respectfully request that the Court issue a warrant authorizing a search of **PANIAGUA'S** person, the **Subject Premises**, and **PANIAGUA's Cell Phone**, as described in Attachment A, for the items listed in Attachment B, and authorizing the seizure and examination of any such items found.

51. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney Gary Sussman. AUSA Sussman advised me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By Telephone

William M. Bergin  
HSI Special Agent

Sworn to telephonically or by other reliable means pursuant to Fed. R. Cr. P. 4.1 at

3:13 ~~am~~ /pm on November 10, 2020.

John Jelderks

HONORABLE JOHN JELDERKS  
United States Magistrate Judge